

IOS路由器作为Easy VPN服务器使用 Configuration Professional配置示例

目录

[简介](#)

[先决条件](#)

[使用的组件](#)

[安装Cisco CP](#)

[运行 Cisco CP 的路由器配置](#)

[要求](#)

[规则](#)

[配置](#)

[网络图](#)

[Cisco CP - Easy VPN服务器配置](#)

[CLI 配置](#)

[验证](#)

[Easy VPN服务器 — show命令](#)

[故障排除](#)

[相关信息](#)

简介

本文档介绍如何使用Cisco Configuration Professional(Cisco CP)和CLI将Cisco IOS®路由配置为[Easy VPN\(EzVPN\)](#)服务器。Easy VPN服务器功能允许远程最终用户使用IP安全(IPsec)与任何Cisco IOS虚拟专用网络(VPN)网关进行通信。集中管理的IPsec策略由服务器“推送”到客户端设备，从而最大限度地减少最终用户的配置。

有关Easy VPN服务器的详细信息，请参阅[Cisco IOS版本12.4T安全连接配置指南库的Easy VPN服务器部分](#)。

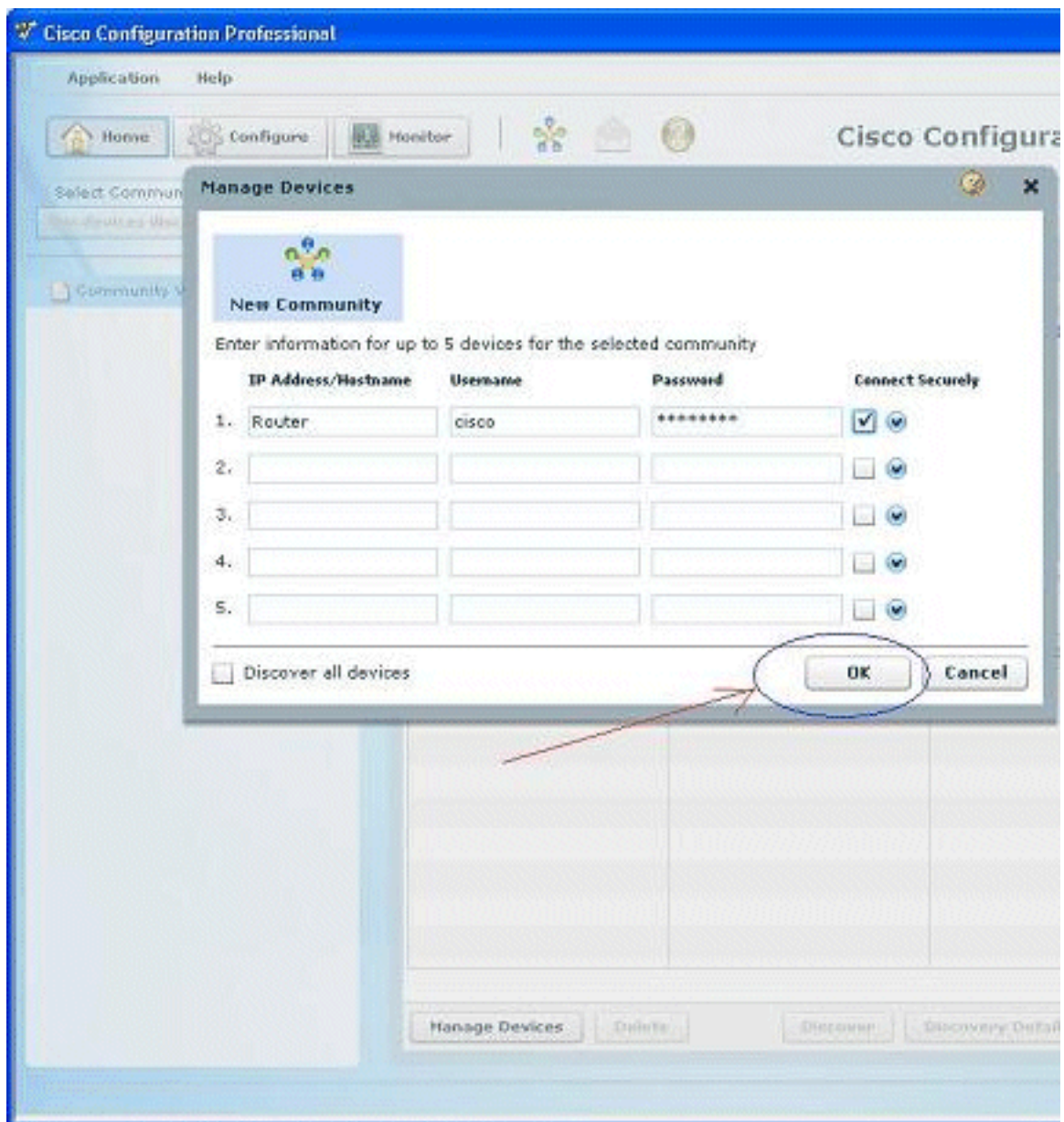
先决条件

使用的组件

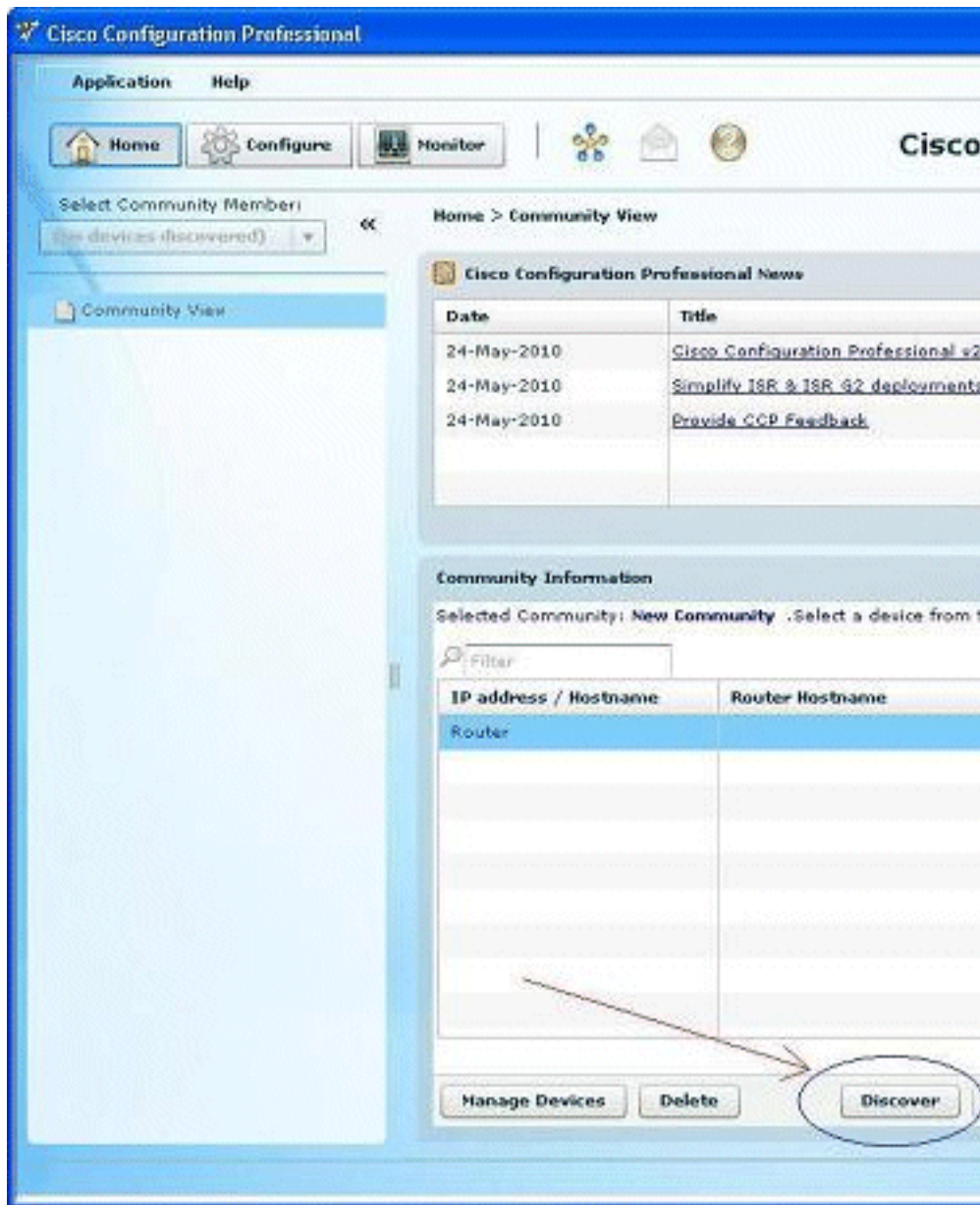
本文档中的信息基于以下软件和硬件版本：

- 配备 Cisco IOS 软件版本 12.4(15T) 的 Cisco 1841 路由器
- Cisco CP 版本 2.1

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。



3. 要发现要配置的设备，请突出显示路由器，然后单击Discover。



注：有关与Cisco CP v2.1兼容的Cisco路由器型号和IOS版本的信息，请参阅兼容的[Cisco IOS版本](#)部分。

注：有关运行Cisco CP v2.1的PC要求的信息，请参阅“系统要求”部分。

[运行 Cisco CP 的路由器配置](#)

要在 Cisco 路由器上运行 Cisco CP，请执行以下配置步骤：

1. 使用 Telnet、SSH 或控制台连接路由器。使用以下命令进入全局配置模式：

```
Router(config)#enable
```

```
Router(config)#
```

2. 如果启用了 HTTP 和 HTTPS 并将其配置为使用非标准端口号，则可跳过此步骤并直接使用已配置的端口号。使用以下 Cisco IOS 软件命令启用路由器 HTTP 或 HTTPS 服务器：

```
Router(config)# ip http server
```

```
Router(config)# ip http secure-server
```

```
Router(config)# ip http authentication local
```

3. 创建一个权限级别为 15 的用户：

```
Router(config)# username privilege 15 password 0
```


注意：将<username>和<password>替换为要配置的用户名和密码。

4. 为本地登录和权限级别15配置SSH和Telnet。

```
Router(config)# line vty 0 4
Router(config-line)# privilege level 15
Router(config-line)# login local
Router(config-line)# transport input telnet
Router(config-line)# transport input telnet ssh
Router(config-line)# exit
```

5. (可选) 启用本地登录以支持日志监控功能：

```
Router(config)# logging buffered 51200 warning
```

要求

本文档假设思科路由器完全运行且已配置为允许思科CP进行配置更改。

有关如何开始使用Cisco CP的完整信息，请参阅[Cisco Configuration Professional入门](#)。

规则

有关文档约定的更多信息，请参考 [Cisco 技术提示约定](#)。

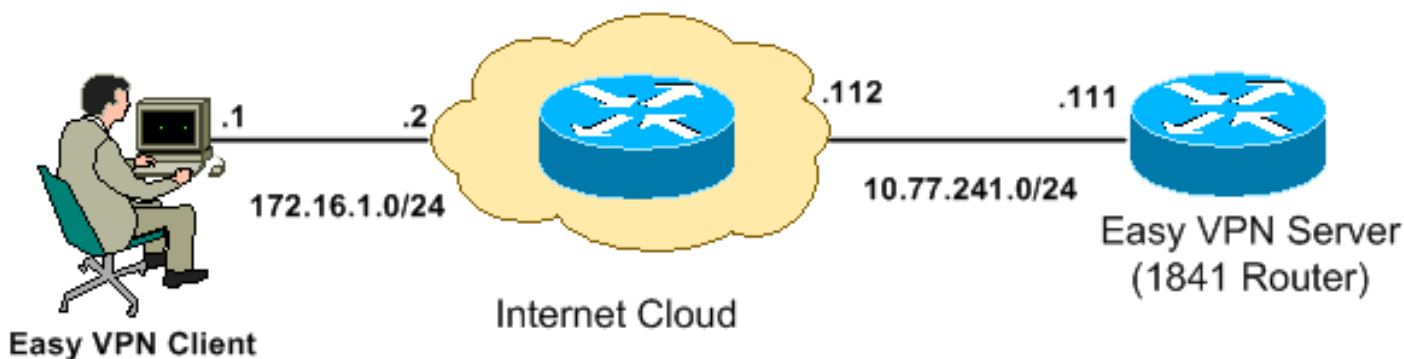
配置

在本部分中，您将了解有关网络中路由器基本设置的配置信息。

注意：使用[命令查找工具](#)([仅限注册客户](#))可获取有关本节中使用的命令的详细信息。

网络图

本文档使用以下网络设置：



注意：此配置中使用的IP编址方案在Internet上不可合法路由。这些地址是在实验室环境中使用的[RFC 1918 地址](#)。

Cisco CP - Easy VPN服务器配置

要将Cisco IOS路由器配置为Easy VPN服务器，请执行以下步骤：

1. 选择Configure > Security > VPN > Easy VPN Server > Create Easy VPN Server，然后单击Launch Easy VPN Server Wizard，以将Cisco IOS路由器配置为Easy VPN服务器

Configure > Security > VPN > Easy VPN Server


VPN

Create Easy VPN Server Edit Easy VPN Server

Cisco CP can guide you through Easy VPN Server configuration tasks.

Use Case Scenario

Configure Easy VPN Server

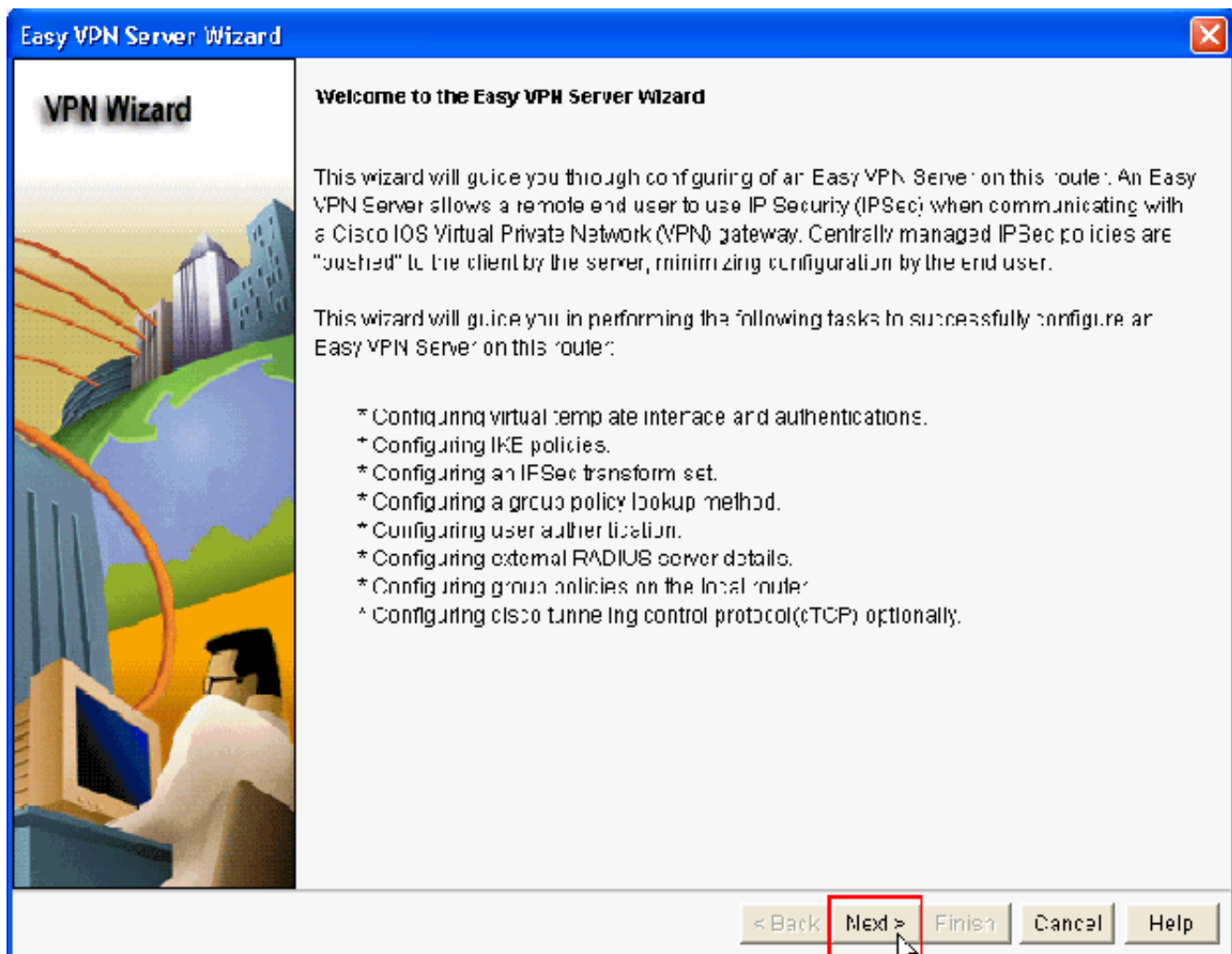


Client 1
Client 2
Internet
Easy VPN server

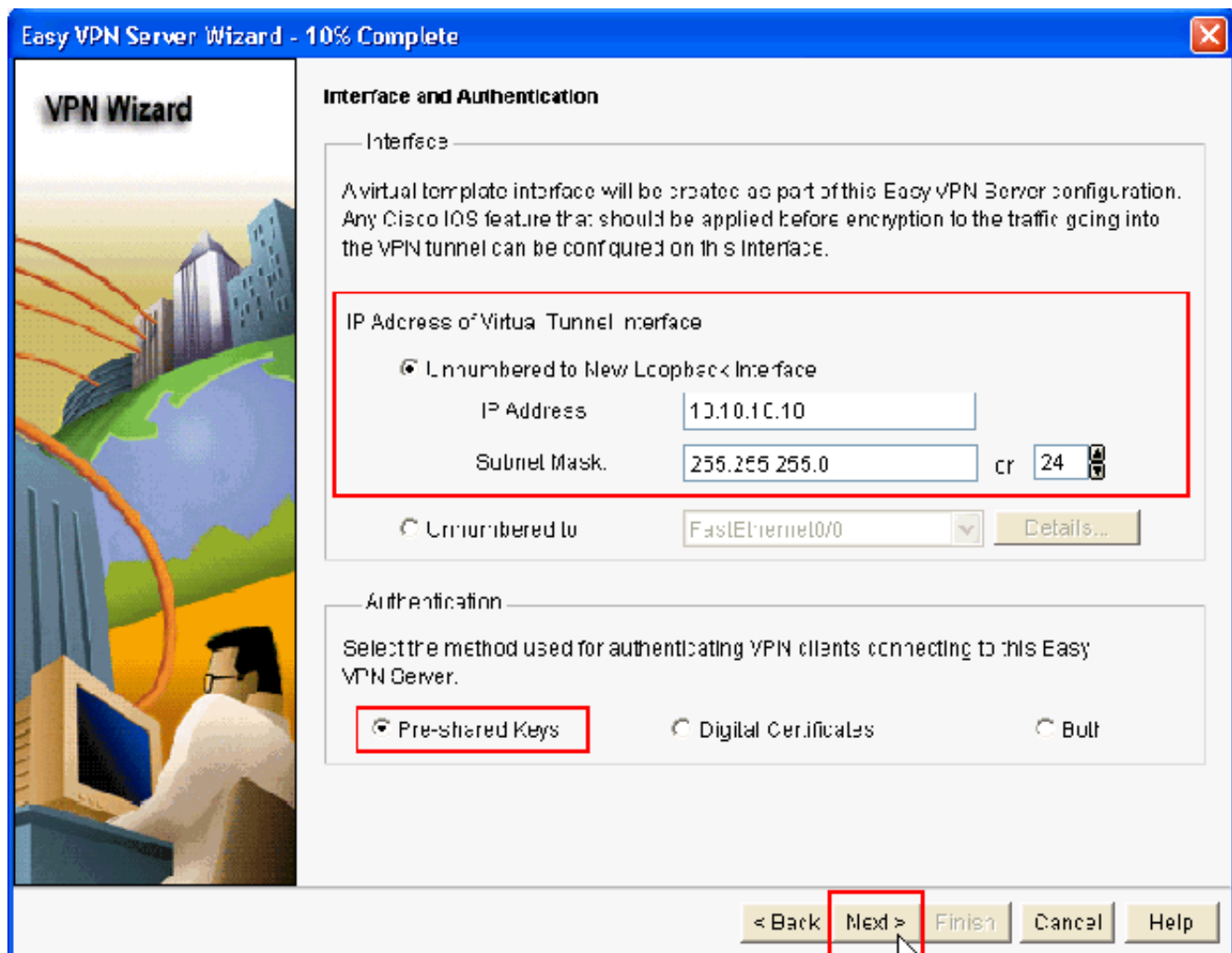
Use this option to configure this router as an Easy VPN Server. To complete the configuration, you must know the different group policies to which the clients can connect and their attributes.

Launch Easy VPN Server Wizard

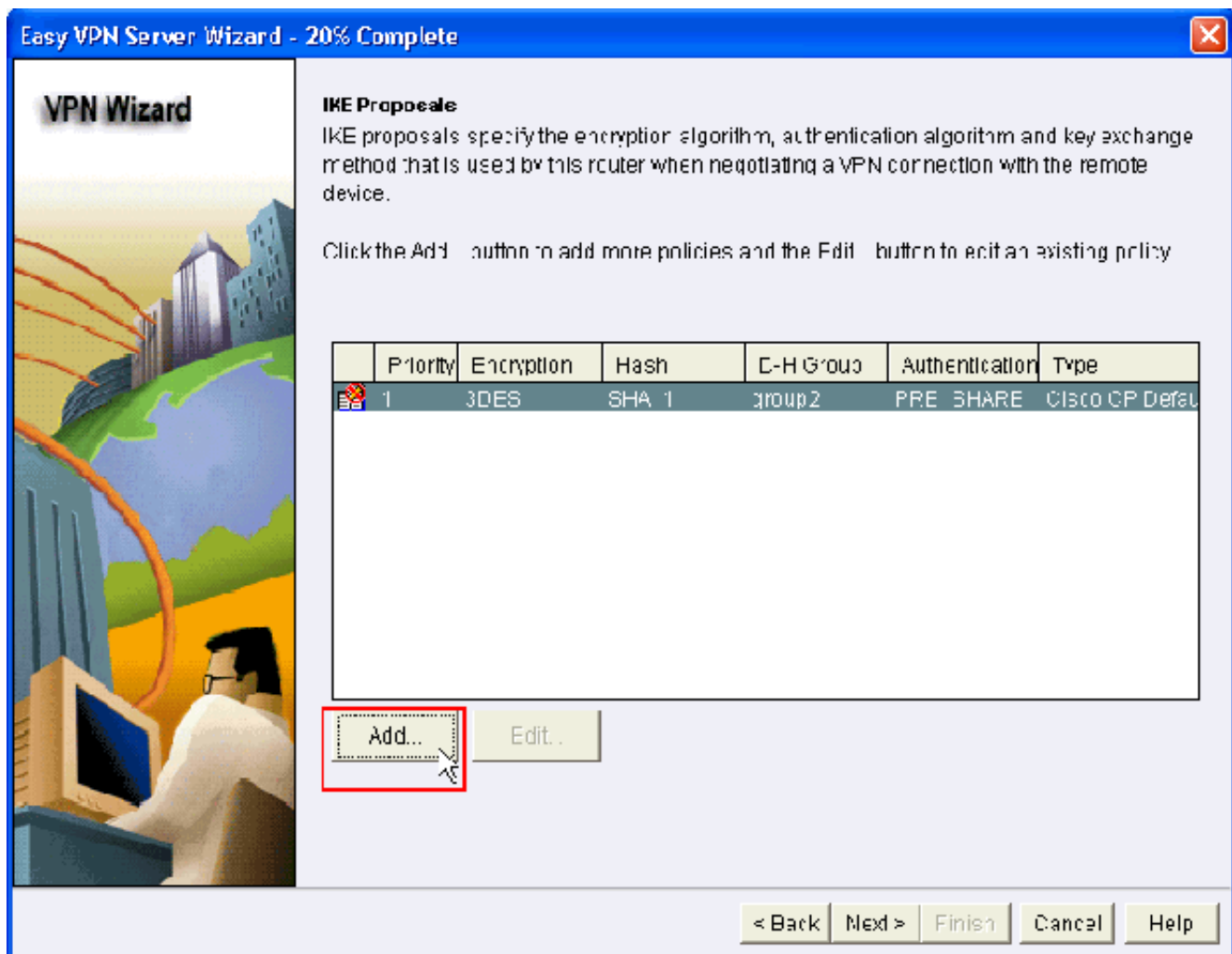
2. 单击Next以继续Easy VPN服务器配置。



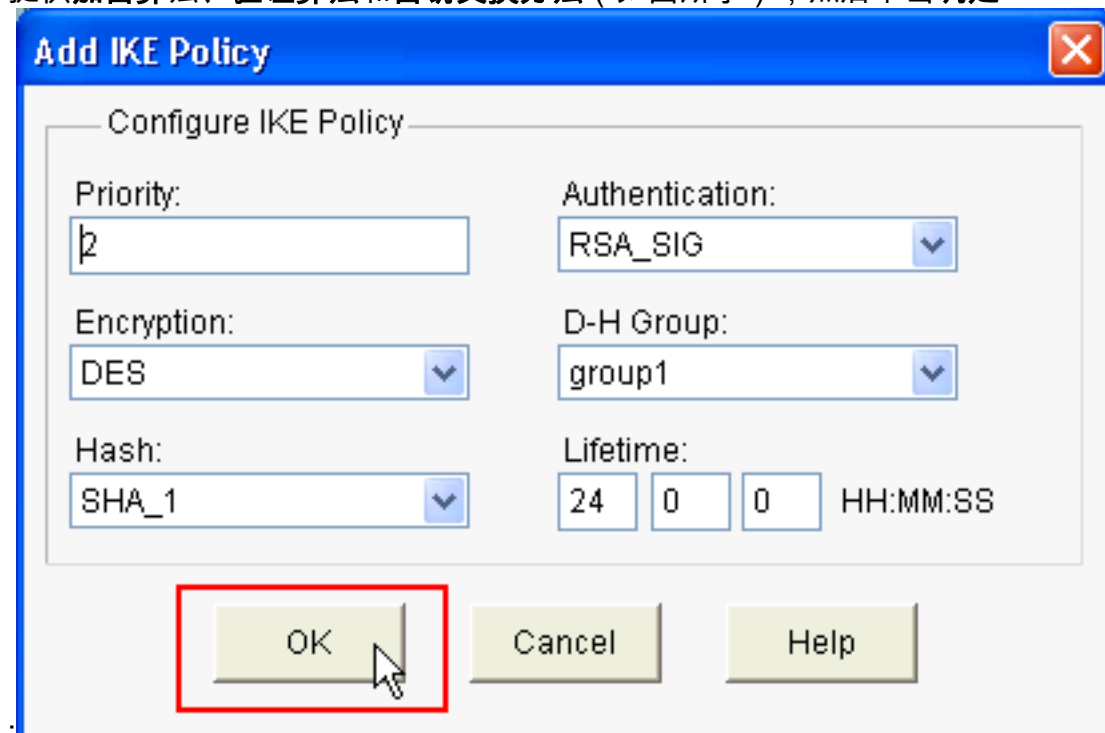
3. 在生成的窗口中，**虚拟接口**将配置为Easy VPN服务器配置的一部分。提供**虚拟隧道接口**的**IP地址**，并选择用于**验证VPN客户端**的身份验证方法。此处，**预共享密钥**是使用的身份验证方法。单击“下一步”：



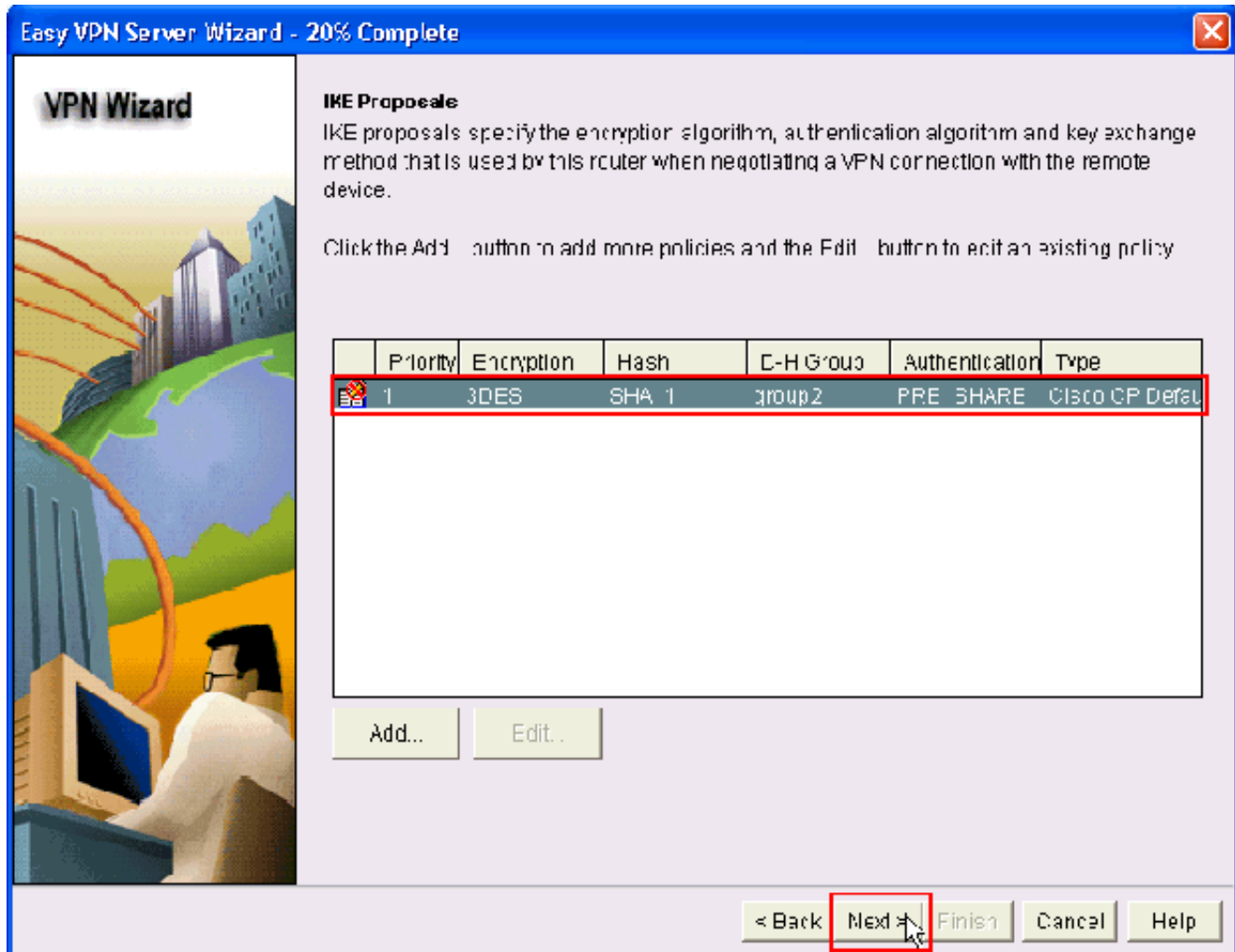
4. 指定此路由器在与远程设备协商时要使用的加密算法、身份验证算法和密钥交换方法。路由器上存在默认IKE策略，如果需要，可使用该策略。如果要添加新的IKE策略，请点击Add。



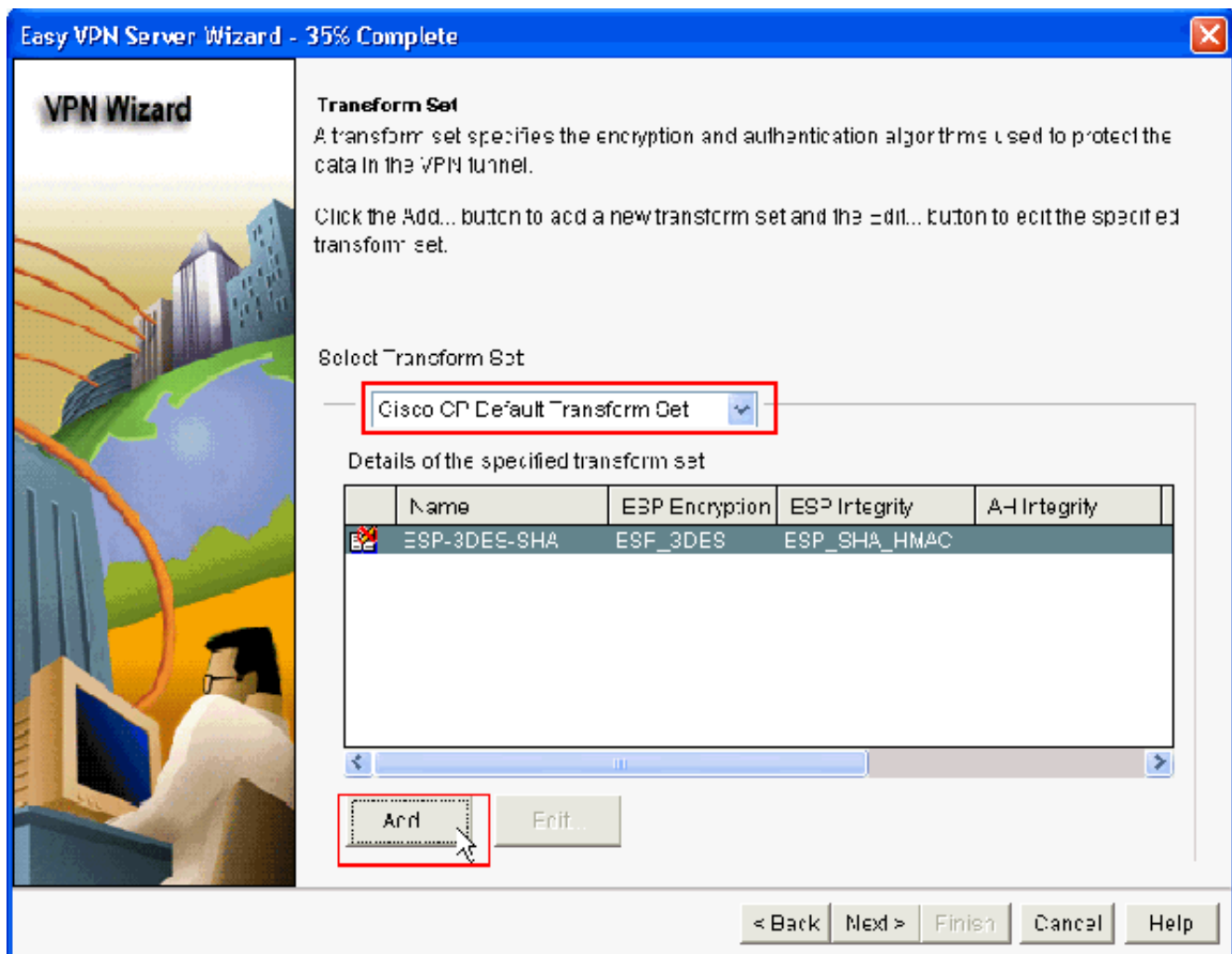
5. 提供加密算法、验证算法和密钥交换方法（如图所示），然后单击确定



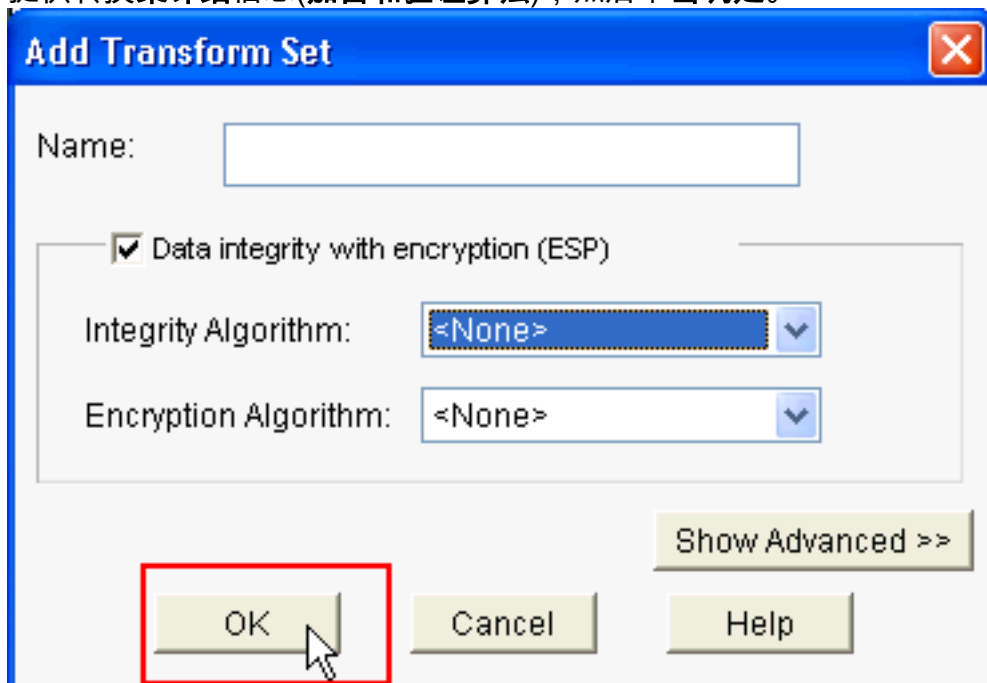
6. 本例中使用默认IKE策略。因此，选择默认IKE策略并单击Next。



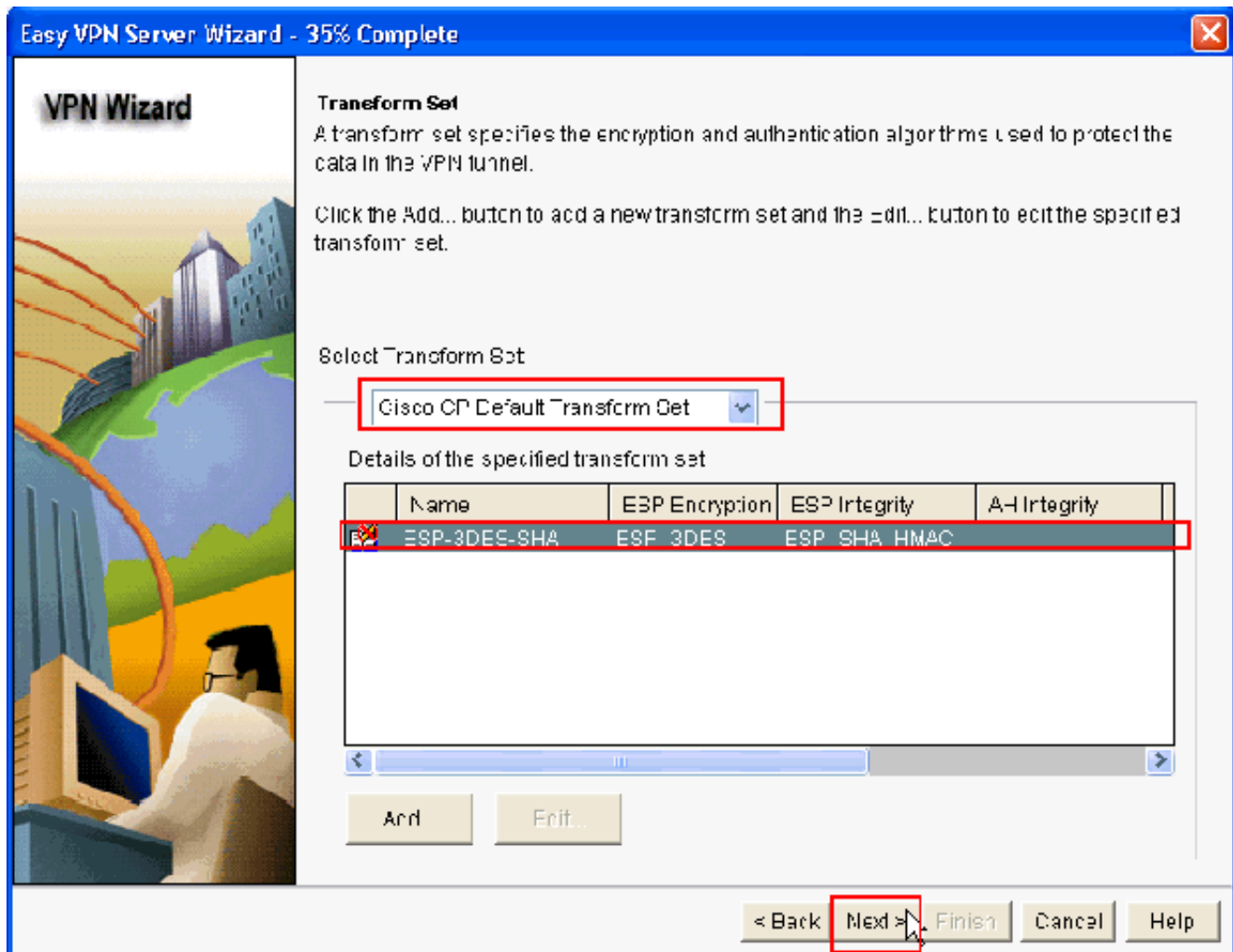
7. 在新窗口中，应提供转换集详细信息。“转换集”指定用于保护 VPN 隧道中的数据的数据的加密算法和验证算法。单击Add提供这些详细信息。单击“添加”并提供详细信息时，可根据需要添加任意数量的转换集。注意：使用Cisco CP配置时，路由器上默认存在CP默认转换集。



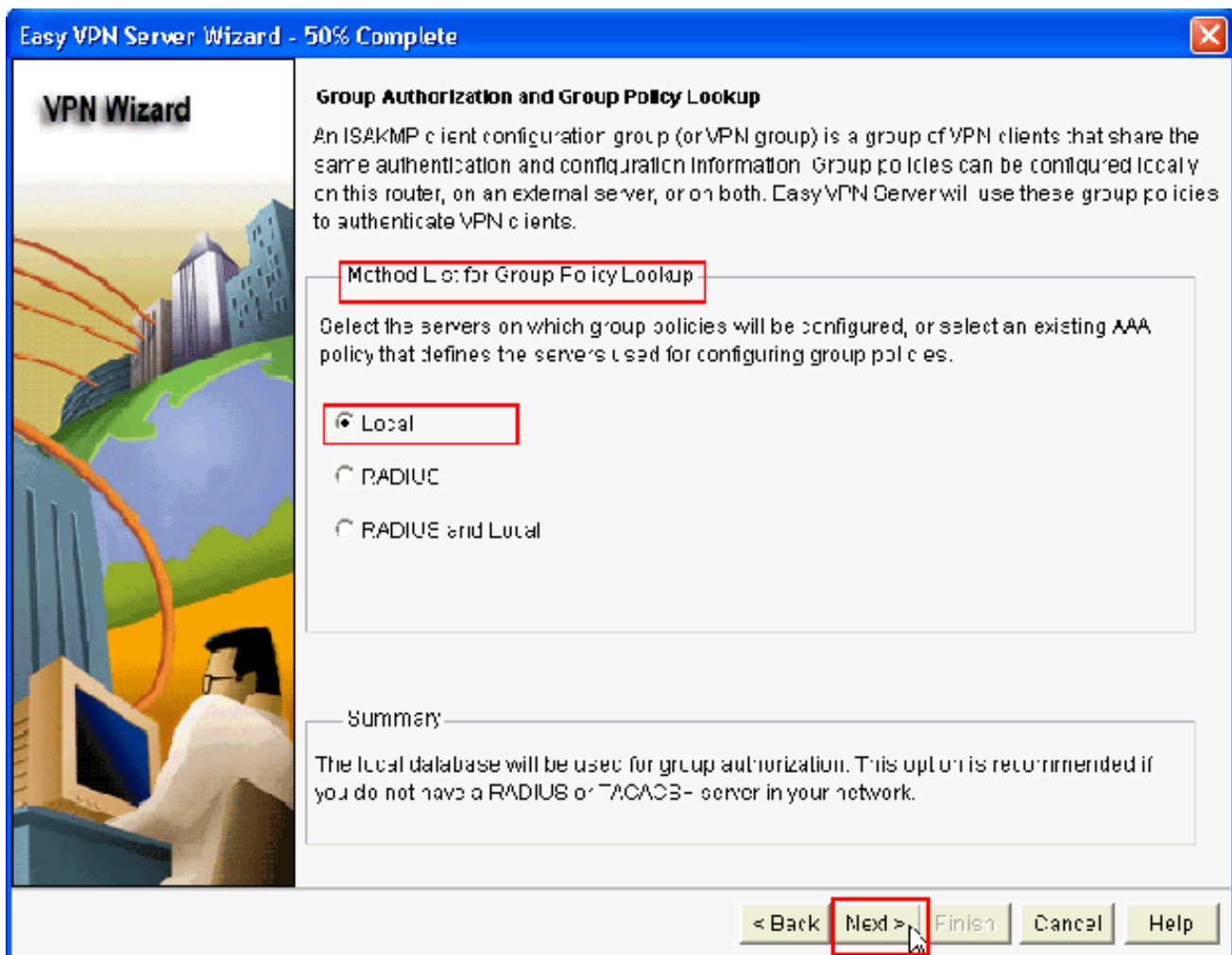
8. 提供转换集详细信息(加密和验证算法)，然后单击确定。



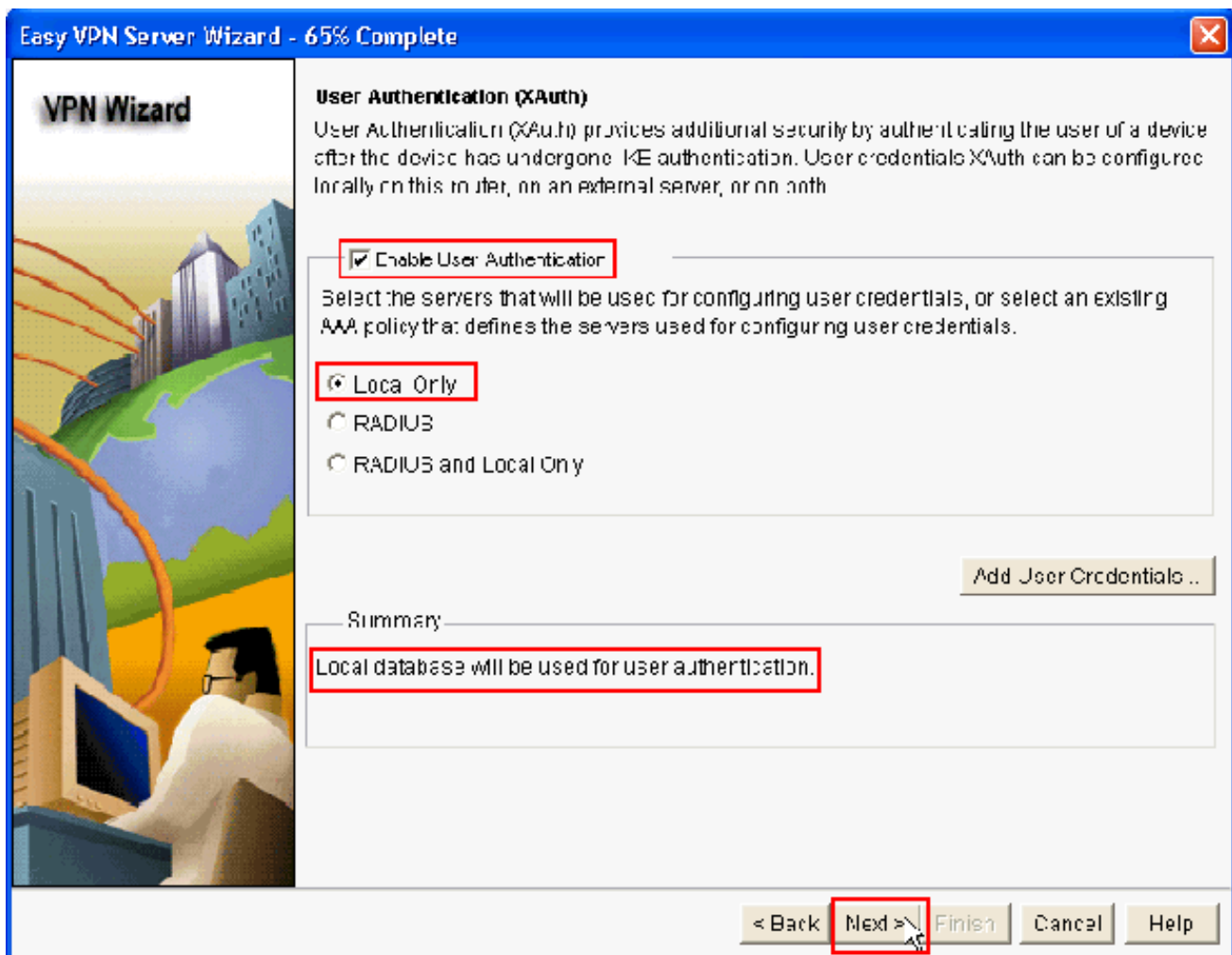
9. 本示例中使用名为CP默认转换集的默认转换集。因此，选择默认的转换集，然后单击“下一步”。



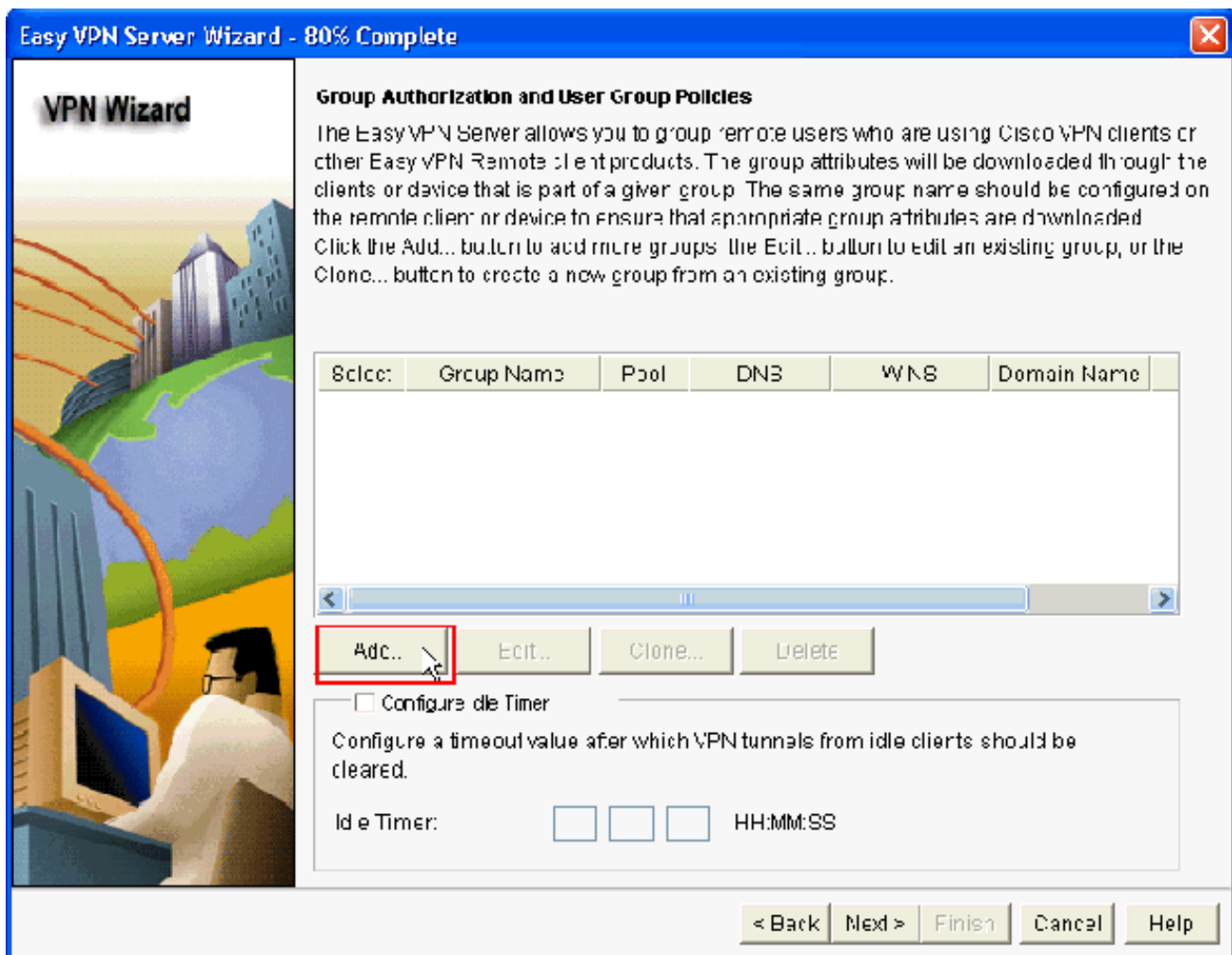
10. 在新窗口中，选择将在其上配置组策略的服务器，该服务器可以是Local或RADIUS，也可以是Local和RADIUS。在本例中，我们使用本地服务器配置组策略。选择“Local”，然后单击“Next”。



11. 在此新窗口中选择要用于用户身份验证的服务器，该窗口可以是仅本地或RADIUS或仅本地和RADIUS。在本示例中，我们使用本地服务器来配置用户身份验证凭据。确保选中Enable User Authentication旁的复选框。选择“仅本地”，然后单击“下一步”。



12. 单击Add以创建新组策略并在此组中添加远程用户。



13. 在“添加组策略”窗口中，在空格中提供组名称，以提供“此组的名称”(本例中为cisco)以及预共享密钥，并提供如图所示的IP池（起始IP地址和结束IP地址）信息，然后单击“确定”。注意：您可以创建新IP池或使用现有IP池（如果存在）。

Add Group Policy [Close]

General | DNS/WINS | Split Tunneling | Client Settings | XAuth Options | Client Update

Name of This Group:

Pre-shared Keys

Specify the key that will be used to authenticate the clients associated with this group.

Current Key: <None>

Enter new pre-shared key:

Reenter new pre-shared key:

Pool Information

Specify a local pool containing a range of addresses that will be used to allocate an internal IP address to a client.

Create a new pool Select from an existing pool

Starting IP address:

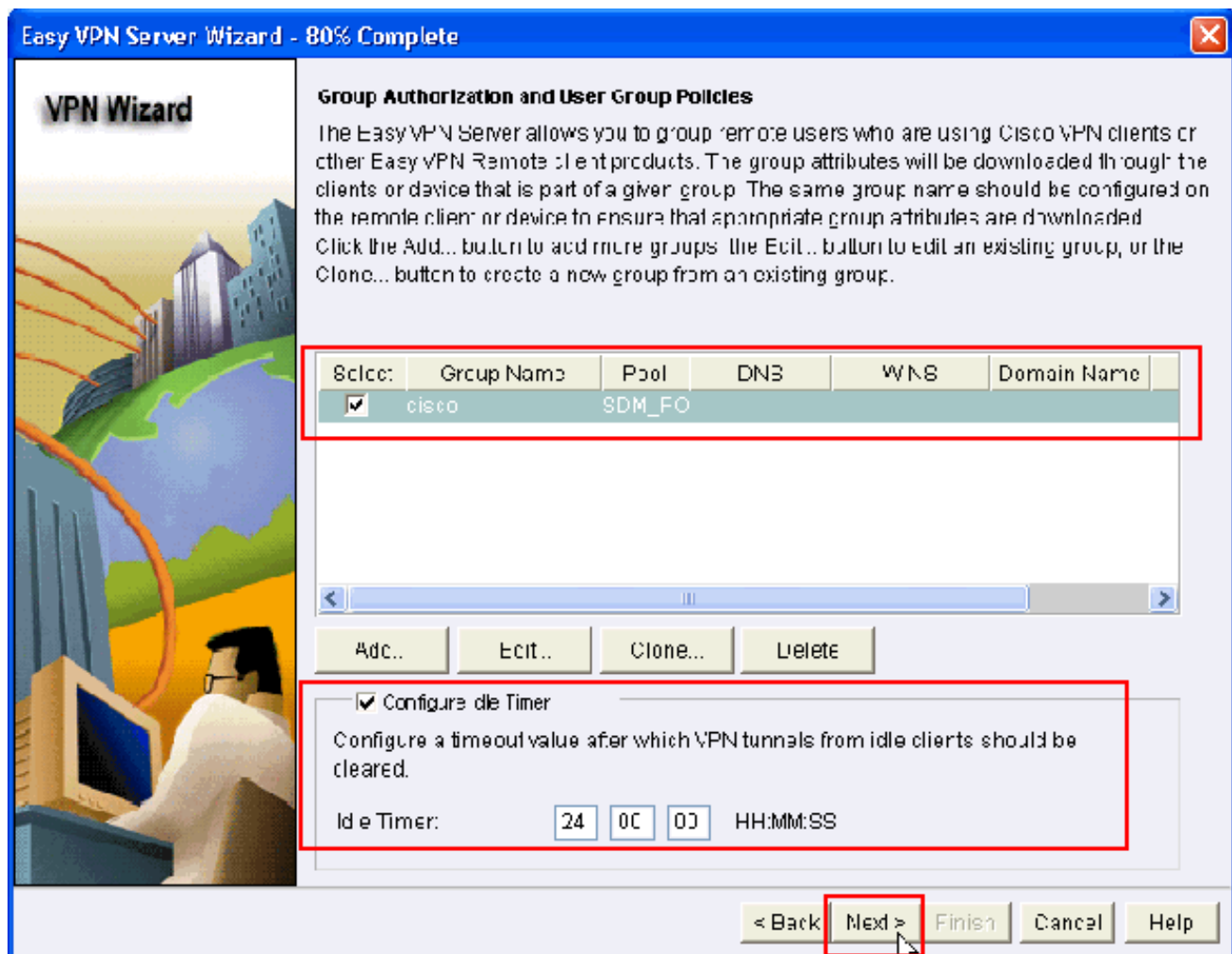
Ending IP address:

Enter the subnet mask that should be sent to the client along with the IP address.

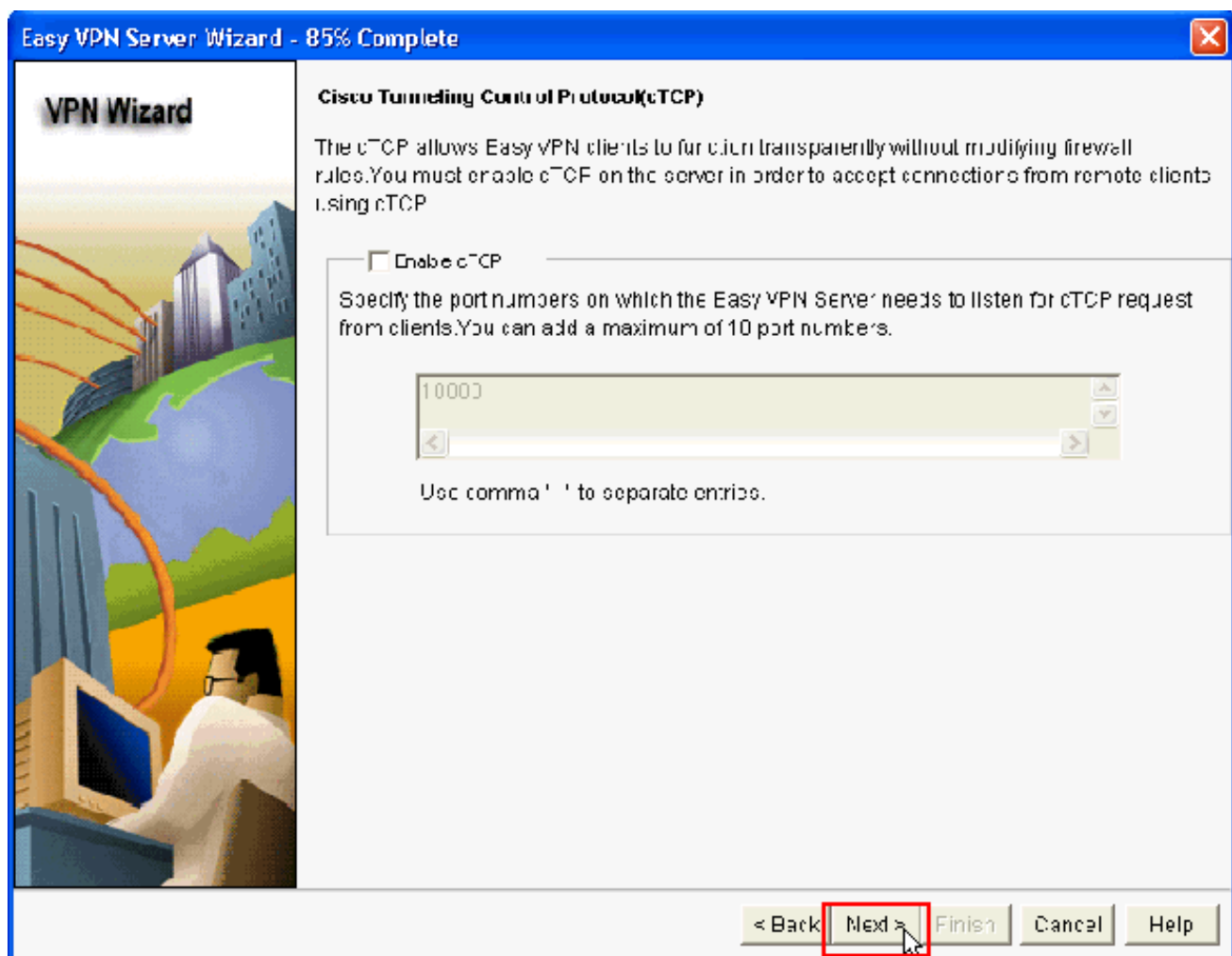
Subnet Mask: (Optional)

Maximum Connections Allowed:

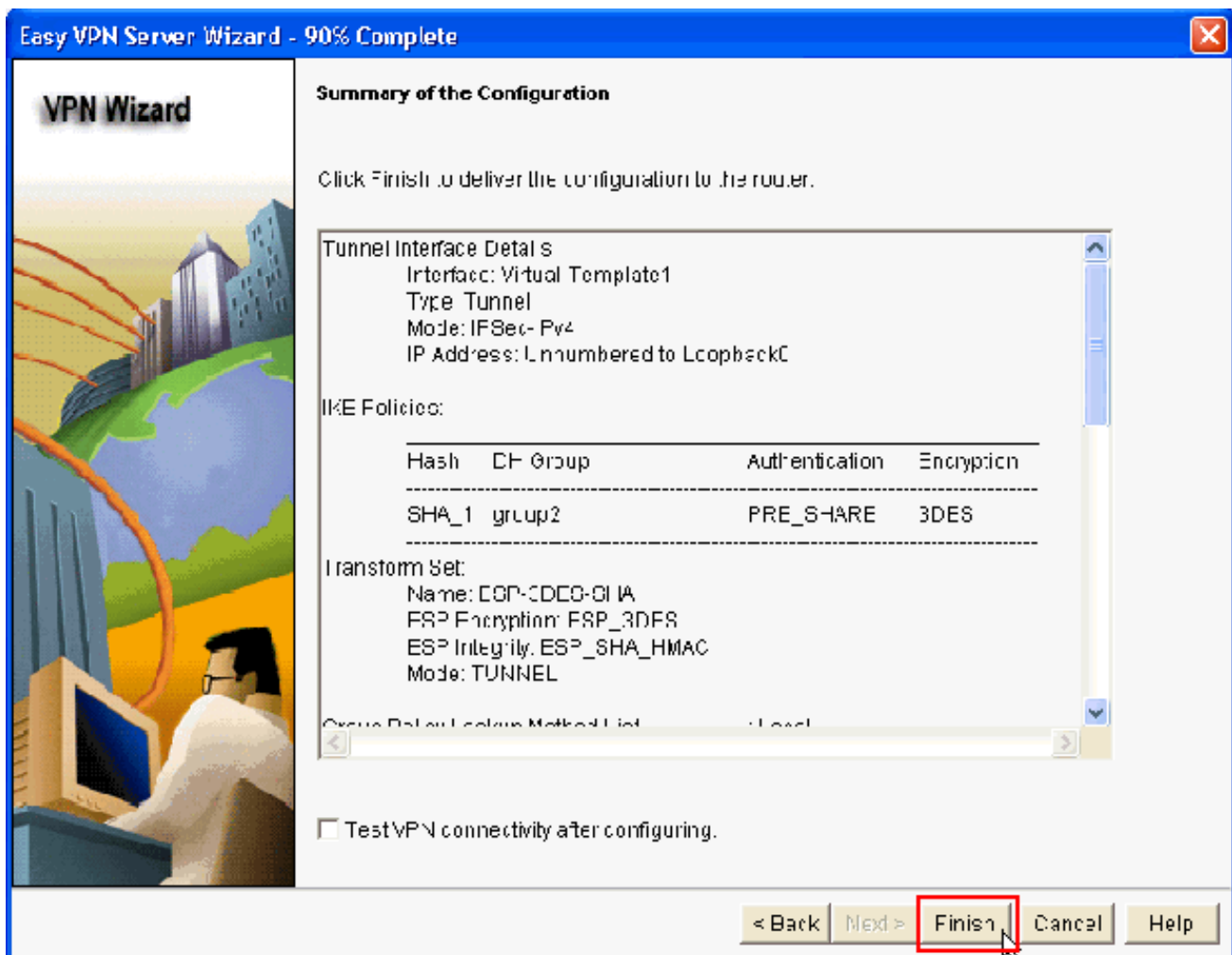
14. 现在，选择名为cisco的新组策略，然后按需单击配置空闲计时器旁的复选框以配置空闲计时器。单击 **Next**。



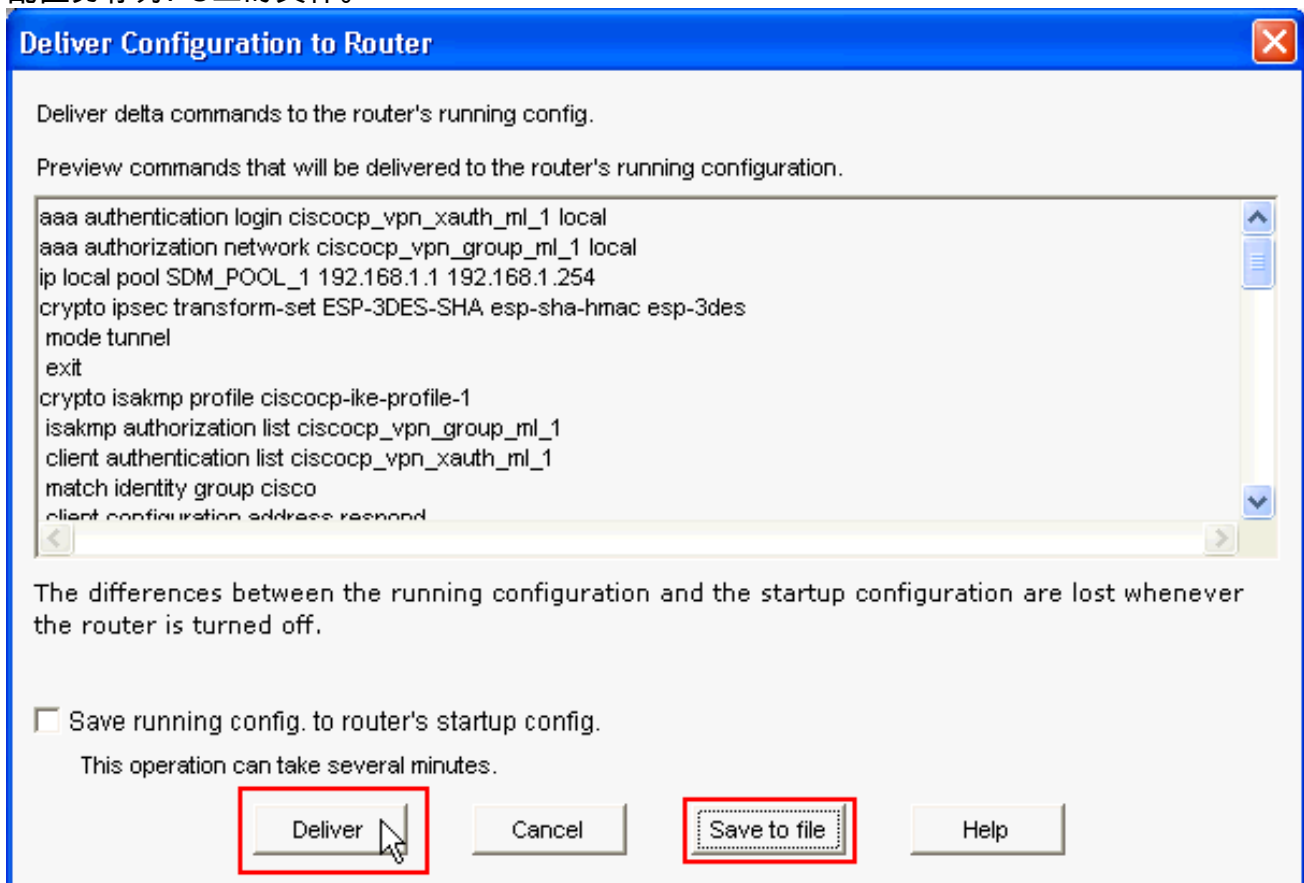
15. 如果需要，请启用思科隧道控制协议(cTCP)。否则，单击**Next**。



16. 查看配置摘要。单击 完成。

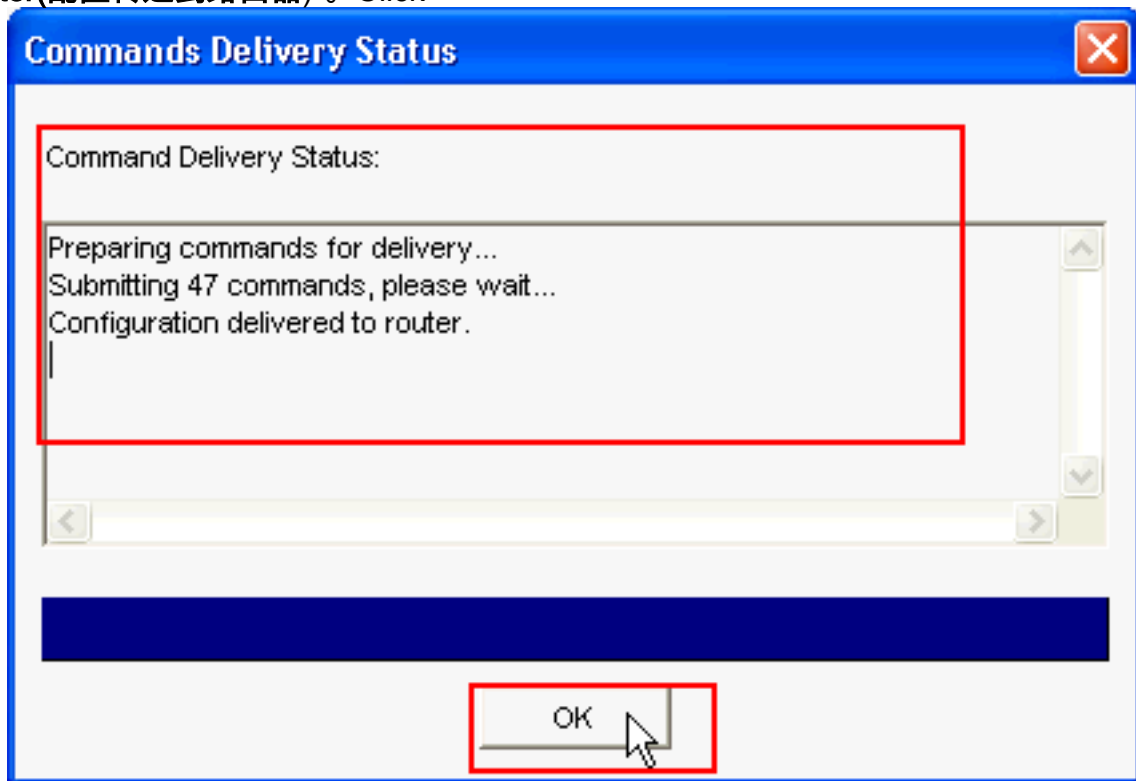


17. 在将配置传送到路由器窗口中，单击传送将配置传送到路由器。您可以单击“保存到文件”，将配置另存为PC上的文件。



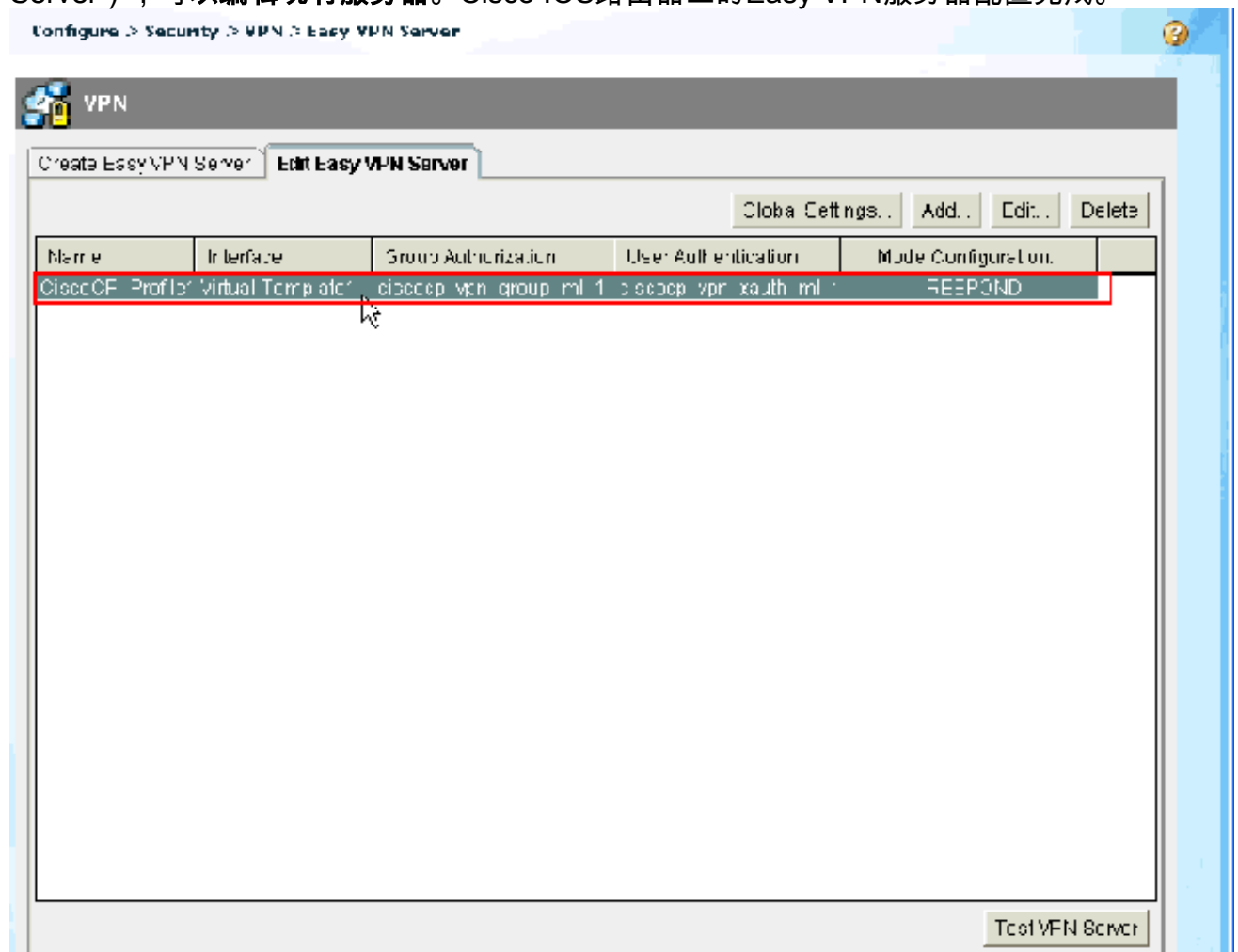
18. 命令传送状态窗口显示命令传送到路由器的状态。它显示为“Configuration delivered to

router(配置传送到路由器)”。Click



OK.

19. 您可以看到新创建的Easy VPN服务器。通过选择Edit Easy VPN Server (编辑Easy VPN Server) , 可以编辑现有服务器。Cisco IOS路由器上的Easy VPN服务器配置完成。



路由器配置

```
Router#show run
Building configuration...

Current configuration : 2069 bytes
! version 12.4 service timestamps debug datetime msec
service timestamps log datetime msec no service
password-encryption hostname Router boot-start-marker
boot-end-marker no logging buffered enable password
cisco !---AAA enabled using aaa newmodel command. Also
AAA Authentication and Authorization are enabled!---! aaa
new-model
!
!
aaa authentication login ciscocp_vpn_xauth_ml_1 local
aaa authorization network ciscocp_vpn_group_ml_1 local
!
!
aaa session-id common
ip cef
!
!
!
!
ip domain name cisco.com
!
multilink bundle-name authenticated
!
!
!--- Configuration for IKE policies. !--- Enables the
IKE policy configuration (config-isakmp) !--- command
mode, where you can specify the parameters that !--- are
used during an IKE negotiation. Encryption and Policy
details are hidden as the default values are chosen.
crypto isakmp policy 1
  encr 3des
  authentication pre-share
  group 2
crypto isakmp keepalive 10
!
crypto isakmp client configuration group cisco
  key cisco123
  pool SDM_POOL_1
crypto isakmp profile ciscocp-ike-profile-1
  match identity group cisco
  client authentication list ciscocp_vpn_xauth_ml_1
  isakmp authorization list ciscocp_vpn_group_ml_1
  client configuration address respond
  virtual-template 1
!
!
!--- Configuration for IPsec policies. !--- Enables the
crypto transform configuration mode, !--- where you can
specify the transform sets that are used !--- during an
IPsec negotiation. crypto ipsec transform-set ESP-3DES-
SHA esp-3des esp-sha-hmac
!
crypto ipsec profile CiscoCP_Profile1
  set security-association idle-time 86400
  set transform-set ESP-3DES-SHA
  set isakmp-profile ciscocp-ike-profile-1
!
```

```

!
!
!--- RSA certificate generated after you enable the !---
ip http secure-server command.

crypto pki trustpoint TP-self-signed-1742995674
  enrollment selfsigned
  subject-name cn=IOS-Self-Signed-Certificate-1742995674
  revocation-check none
  rsakeypair TP-self-signed-1742995674

!--- Create a user account named cisco123 with all
privileges.

username cisco123 privilege 15 password 0 cisco123
archive
  log config
  hidekeys
!
!
!--- Interface configurations are done as shown below---
! interface Loopback0 ip address 10.10.10.10
255.255.255.0 ! interface FastEthernet0/0 ip address
10.77.241.111 255.255.255.192 duplex auto speed auto !
interface Virtual-Templat1 type tunnel ip unnumbered
Loopback0 tunnel mode ipsec ipv4 tunnel protection ipsec
profile CiscoCP_Profile1 ! !--- VPN pool named
SDM_POOL_1 has been defined in the below command---! ip
local pool SDM_POOL_1 192.168.1.1 192.168.1.254

!--- This is where the commands to enable HTTP and HTTPS
are configured. ip http server ip http authentication
local ip http secure-server ! ! ! ! control-plane ! line
con 0 line aux 0 !--- Telnet enabled with password as
cisco. line vty 0 4 password cisco transport input all
scheduler allocate 20000 1000 ! ! ! ! end

```

验证

Easy VPN服务器 — show命令

使用本部分可确认配置能否正常运行。

- **show crypto isakmp sa** - 显示对等体上的所有当前 IKE SA。

```
Router#show crypto isakmp sa
```

```
IPv4 Crypto ISAKMP SA
dst          src          state          conn-id slot status
10.77.241.111 172.16.1.1   QM_IDLE       1003     0  ACTIVE
```

- **show crypto ipsec sa** - 显示对等体上的所有当前 IPsec SA。

```
Router#show crypto ipsec sa
```

```
interface: Virtual-Access2
  Crypto map tag: Virtual-Access2-head-0, local addr 10.77.241.111

protected vrf: (none)
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (192.168.1.3/255.255.255.255/0/0)
current_peer 172.16.1.1 port 1086
  PERMIT, flags={origin_is_acl,}
```

```
#pkts encaps: 28, #pkts encrypt: 28, #pkts digest: 28
#pkts decaps: 36, #pkts decrypt: 36, #pkts verify: 36
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 2

local crypto endpt.: 10.77.241.111, remote crypto endpt.: 172.16.1.1
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
current outbound spi: 0x186C05EF(409732591)

inbound esp sas:
spi: 0x42FC8173(1123844467)
transform: esp-3des esp-sha-hmac
```

故障排除

[命令输出解释程序 \(仅限注册用户 \) \(OIT\) 支持某些 show 命令。](#) 使用 OIT 可查看对 show 命令输出的分析。

注意：在发出debug命令之前，[请参阅](#)有关debug命令的重要信息。

相关信息

- [IPsec 协商/IKE 协议](#)
- [Cisco Configuration Professional 快速入门指南](#)
- [思科产品支持页 - 路由器](#)
- [技术支持和文档 - Cisco Systems](#)